REPRINT

R&C risk & compliance

IDENTIFYING AND PREPARING FOR PRIVACY AND CYBER SECURITY RISKS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2021 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

SheppardMullin

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

PERSPECTIVES

IDENTIFYING AND PREPARING FOR PRIVACY AND CYBER SECURITY RISKS

BY **LIISA THOMAS**
> SHEPPARD MULLIN RICHTER & HAMPTON LLP

Cyber attacks have become big business for threat actors and companies are working hard to be prepared. At the same time, privacy regulations are changing and increasing, and enforcement of privacy laws is similarly on the upswing. As companies use more sophisticated technologies, like artificial intelligence and biometrics, their cyber security risks and privacy compliance obligations increase.

The Federal Trade Commission (FTC), for example, has emphasised to companies that it will be looking closely to see if companies are taking care to avoid discriminatory outcomes, using correct datasets, and otherwise using artificial intelligence in fair and equitable ways. In other words, not using it to engage in unfair and deceptive practices in violation of the FTC Act.

The European Data Protection Board (EDPB) has made similar cautions to companies. Meanwhile, organisations know that threat actors are looking for opportunities to exploit technical vulnerabilities. Phishing attacks, ransomware demands and other cyber crimes are on the rise.

In light of these risks, what can companies do? There are four key steps that every company can implement to prepare – and remain vigilant – in this increasingly risky world.

Acknowledge that not all risks are the same

Companies faced with potential cyber attacks or trying to prepare for constantly changing laws will often jump immediately into action. These include updating policies, implementing operating procedures to execute on those policies, strengthening internal controls and auditing compliance. These steps are of course helpful, and many are required by law. They often, though, may only help with preventable risks.

However, these are only one type of risk, according to management theorists Robert Kaplan and Anette Mikes. Another type of risk, strategic, involves weighing the amount of risk a company is willing to undertake. Like preventable risks, strategic risks are typically ones that arise in the face of a known threat.

The situations companies are facing today – with multiple potential cyber attacks arriving at unknown times, in unknown ways, by unknown threat actors – fall into a third category of risk: unpredictable and unknown risks. To manage these risks, companies need different tools in their toolbox. For Kaplan and Mikes, tools include identifying these risks when they happen (often easier said than done) and mitigating the potential negative impact.

A written policy may not be able to prepare a company for every possible situation, but tabletop exercises that focus on teamwork, rather than on preparing for a specific type of incident, could. Other tools include short checklists, along the lines used by pilots. In other words, highly skilled individuals who need a simple reminder set off of which to work. Some data incidents may arise from risks that fall into multiple categories, so developing multiple mitigation strategies can be important.

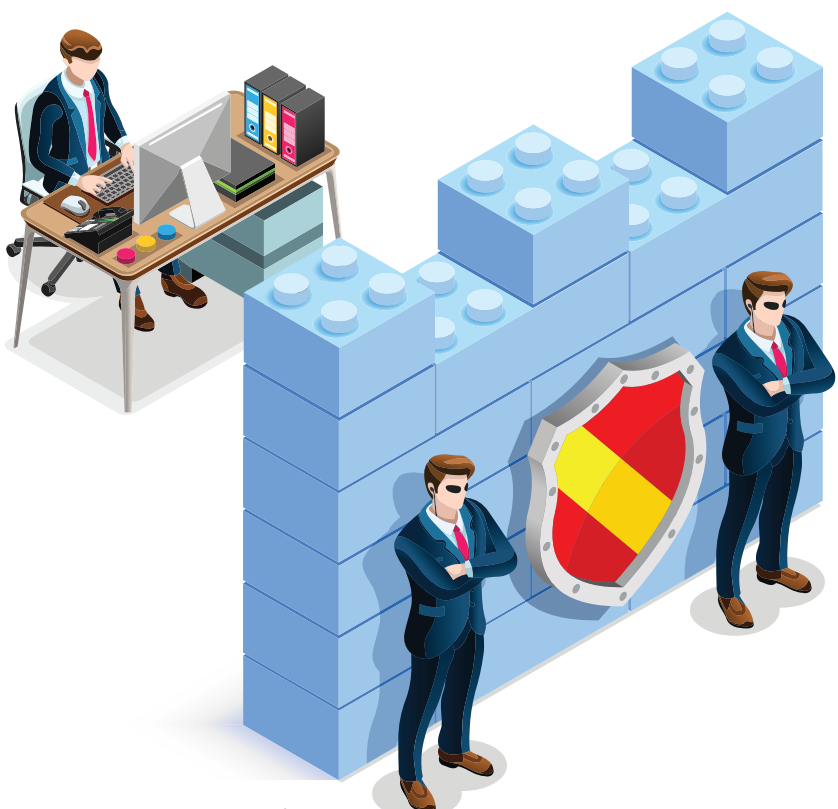
> **"As companies use more sophisticated technologies, like artificial intelligence and biometrics, their cyber security risks and privacy compliance obligations increase."**

Begin from a place of customisation

The second step companies can take, and a related one, is customising their privacy compliance approach to their own company. Privacy and data security laws place bespoke obligations on companies. Privacy notices need to describe the company's practices. Data security laws anticipate

policies that are designed for the risks that the company faces.

To customise a programme, the start is not taking an off-the-shelf policy or copying the approach of a competitor. Instead, privacy professionals will look at their organisation's strategic needs. What are the goals of the organisation? What is the current environment in which it is operating? What challenges does it face? What are its existing strengths? These needs are then weighed against the company's strengths, weaknesses, opportunities and threats.



Diligence to identify strengths and weaknesses would include tangible areas like the types of information a company collects and how it uses it, the types of security measures it uses and the like. It would also, though, include 'intangibles' like 'How well does our team work together?' and 'Who are the key decision makers (that would be calling the shots during a data incident)?' Diligence to identify external opportunities and threats include an understanding of anticipated legal developments, current enforcement activities, as well as an analysis of the competitive landscape. Once a company has a good understanding of its situation, it is in a better position to prepare for both known and unknown risks, and can identify both gaps and opportunities.

Be strategic in remediation approaches

Third, once a company has completed the prior step, it can begin to develop a strategic and bespoke approach to remediation. A strategic programme is one that takes into account and supports the underlying business needs and goals and is designed around that reality. A strategic programme is also one that is

implementable, not aspirational. It is one that can be easily understood by company personnel (and thus followed), and training to adhere to the programme is achievable.

A strategic programme is one that takes into account the fact that corporate activities are ever changing, as are privacy and data security laws. A strategic programme anticipates that modifications will be needed, and is not designed with a 'set it and forget it' approach.

Borrowing from strategic management tools like Robert Kaplan and David Norton's 'scorecard', the legal and compliance team can think through the personnel and infrastructure needed to reach its strategic goals. To help underscore the need for those resources, it can then reflect on what the impact will be on its 'consumers' (i.e., the internal stakeholders whom it supports), and, similarly, how having those resources will support the company's financial goals. This is a value-add approach, and typically one that is more palatable to business leaders. It focuses on how privacy compliance can help the company, and the bottom line.

Make the programme adaptable

Finally, a customised and strategic approach to risk will be most effective if it is adaptive. Instead of needing constant modification as laws or practices change, it should grow and adapt as those inevitabilities occur. An adaptive privacy programme, most critically, is both aligned with and supportive of the organisation's underlying mission, vision and goals. Such a programme is bespoke to the organisation, and avoids extraneous elements or those that do not account for the company's ultimate activities and needs. The programme also takes into account both regulatory and litigation risk, and is flexible enough to adapt as those change. Finally, it is a programme that the organisation can get behind and support. From line managers to senior leadership, it is a programme that is digestible and around which people can easily be trained.

Conclusion

Companies would be well served to take extra time and effort at the beginning of their compliance efforts to align their approach to their underlying business needs and goals. At the same time, they can evaluate the actual risks facing their organisation; recognising that not all risks are the same. For unknown and uncontrollable risks, an adaptive team approach may result in a better outcome than relying solely on updated policies and check-the-box trainings. R&C

Liisa M. Thomas
Partner
Sheppard Mullin
T: +1 (312) 499 6335
E: lmthomas@sheppardmullin.com